## IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for network security comprising:

receiving a request from a remote address at a host;

observing a behavioral pattern of packets associated with the request;

authenticating the remote address based on the behavioral pattern of packets associated with the request; and

enabling access to the host by the remote address for a configurable time period if the remote address is authenticated;

wherein the authentication is based at least in part on a determination that the observed behavioral pattern of packets matches a properly authenticated pattern comprising a plurality of connection requests, probes, or scans received in a specific sequence corresponding to the pattern; and wherein enabling access comprises allowing the remote address to establish, through a connection request received during the configurable period of time, a connection with the host via a port with which the request is associated and closing the port after expiration of the configurable period of time; wherein closing the port after the expiration of the configurable period of time results in connection requests received after the port has been closed being rejected while allowing the remote address to continue to communicate with the host, even after the port has been closed to new connection requests, through the connection established through the connection request received during the configurable period of time.

2. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 further including preventing a response from being sent to the remote address.

3. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein receiving a request from a remote address at the host further includes receiving a probe.

4. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes recording data received at the host.

5. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes matching the pattern to a list.

6. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein observing a pattern associated with the request further includes recording a sequence.

7. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes comparing the pattern to a list.

8. (Cancelled)

9. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes preventing a response being sent to the remote address if the remote address fails to authenticate.

10. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the pattern associated with the request further includes denying access to the host if the remote address fails to authenticate.

11. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein authenticating the remote address based on the

pattern associated with the request further includes sending a message to the remote address if the request fails to authenticate.

12. (Cancelled)

13. (Original) A method for preventing network discovery of a system services configuration as recited in claim 1 wherein enabling access to the host by the remote address further includes implementing a handshake between the remote address and the host.

14. (Currently Amended) A system for preventing network discovery of a system services configuration comprising:

a port for receiving a request from a remote address;

a listening module for observing a behavioral pattern of packets associated with the request; and

an agent for authenticating the remote address and the behavioral pattern of packets associated with the request and enabling access to the port if the behavioral pattern of packets associated with the request is authenticated;

wherein the authentication is based at least in part on a determination that the observed behavioral pattern of packets matches a properly authenticated pattern comprising a plurality of connection requests, probes, or scans received in a specific sequence corresponding to the pattern; and wherein enabling access comprises allowing the remote address to establish, through a connection request received during the configurable period of time, a connection with the host via a port with which the request is associated and closing the port after expiration of the configurable period of time; wherein closing the port after the expiration of the configurable period of time results in connection requests received after the port has been closed being rejected while allowing the remote address to continue to communicate with the host, even after the port has been closed to new connection requests, through the connection established through the connection request received during the configurable period of time.

15. (Cancelled)

16. (Currently Amended) A computer program product for preventing network discovery of a system services configuration, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

receiving a request from a remote address at a port;

observing a behavioral pattern of packets associated with the request;

authenticating the request from the remote address based on the behavioral pattern of packets associated with the request; and

enabling access by the remote address to the port to initiate a connection if the request is authenticated;

wherein the authentication is based at least in part on a determination that the observed behavioral pattern of packets matches a properly authenticated pattern comprising a plurality of connection requests, probes, or scans received in a specific sequence corresponding to the pattern; and wherein enabling access comprises allowing the remote address to establish, through a connection request received during the configurable period of time, a connection with the host via a port with which the request is associated and closing the port after expiration of the configurable period of time; wherein closing the port after the expiration of the configurable period of time results in connection requests received after the port has been closed being rejected while allowing the remote address to continue to communicate with the host, even after the port has been closed to new connection requests, through the connection established through the connection request received during the configurable period of time.

17. (Previously Presented) The system of claim 14 wherein the agent is configured to prevent a response from being sent to the remote address.

18. (Previously Presented) The system of claim 14 wherein receiving a request from a remote address at the host further includes receiving a probe.

19. (Previously Presented) The system of claim 14 further including a recording module for recording the received pattern.

20. (Previously Presented) The system of claim 14 further including a matching module for matching the observed pattern to a list.

21. (Previously Presented) The system of claim 14 wherein authenticating the remote address based on the pattern associated with the request further includes comparing the pattern to a list.

22. (Previously Presented) The system of claim 14 wherein authenticating the remote address based on the pattern associated with the request further includes preventing a response being sent to the remote address if the remote address fails to authenticate.